# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The UDP protocol reveals that the UDP request sent to port 53 was unsuccessful and unreachable, indicating that resolution failed. Port 53 is typically used for DNS services, which are responsible for translating domain names into IP addresses.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “udp port 53 unreachable” This means that DNS request could not be delivered  The port noted in the error message is used for: DNS service  That the IP address for the domain “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)” did not go through to the DNS service. There was no service listening to the receiving DNS port 53. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The first incident occurred at 13:24:32.1925751 when the team reported that a website was not responding correctly by getting an error of destination port unreachable. The IT department was aware of this situation and responded. They took action by analyzing the situation. They used the network analyzer tool tcpdump to verify and analyze the network traffic. By analyzing the loading of the website we have discovered that DNS were not responding correctly. DNS is responsible for translating domain names into IP addresses in order to send and receive requests of a website server. UDP port 53 was unreachable due to the DNS service which was not responding. The team attempted three times to access the website by analyzing the behavior of the network. There might be a service down of DNS and this can be the cause of this situation. The security engineers are after this situation trying to resolve this issue. |